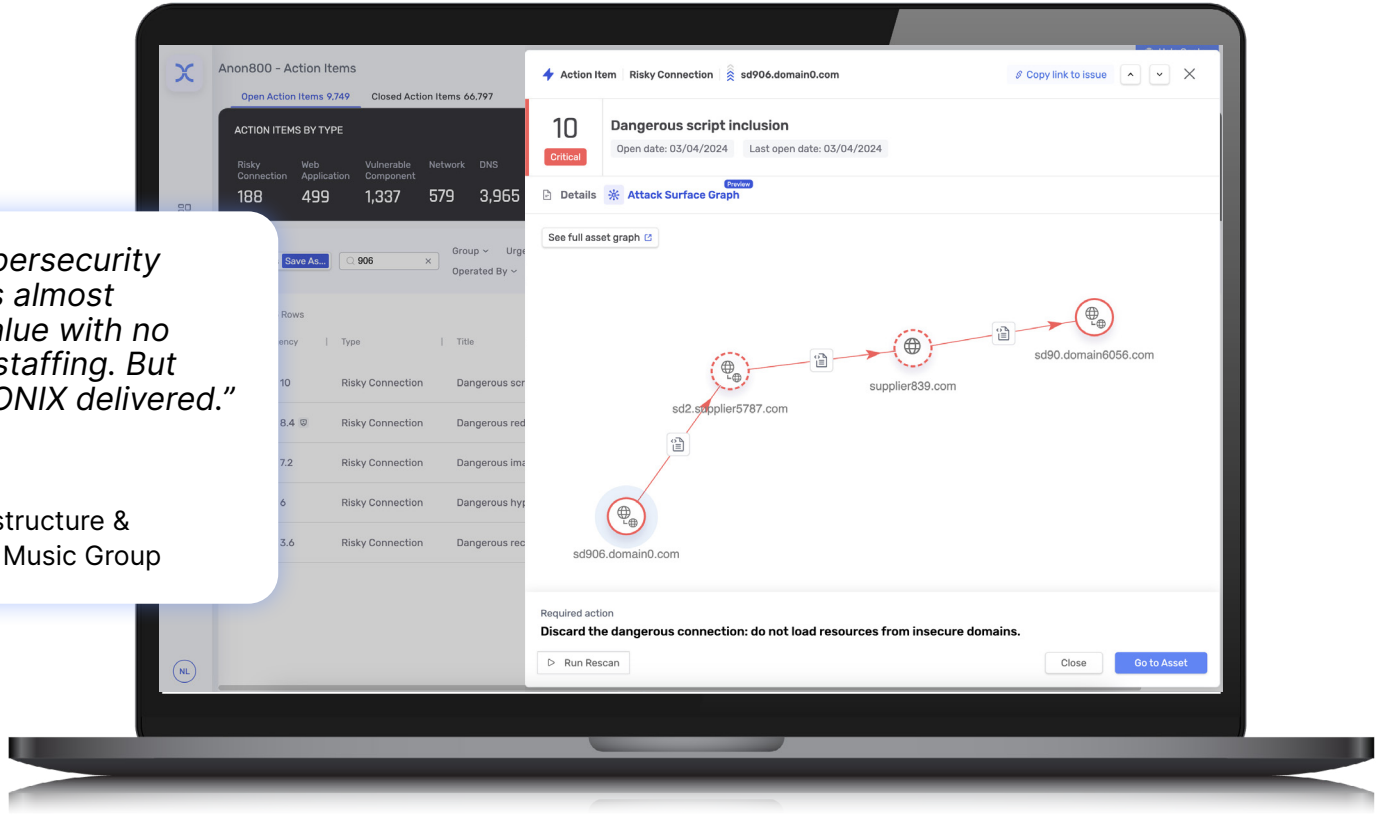
IONIX

DATASHEET

IONIX EXTERNAL EXPOSURE MANAGEMENT

EXPOSE THREATS ACROSS YOUR REAL ATTACK SURFACE



"It's rare to find a cybersecurity solution that delivers almost immediate time to value with no impact on technical staffing. But that's exactly what IONIX delivered."

John Remo
SVP Global Cloud / Infrastructure & Cybersecurity at Warner Music Group

THE FOUR PILLARS OF THE EXPOSURE MANAGEMENT CHALLENGE

In today's complex digital landscape, organizations struggle to protect an ever-expanding attack surface while operating with limited security resources.

IONIX revolutionizes exposure management by addressing four critical challenges that plague modern security teams:

BLIND SPOTS

As digital footprints expand across multiple environments, dangerous blind spots emerge that traditional security tools miss.

SILOED ATTACK SURFACE VIEWS

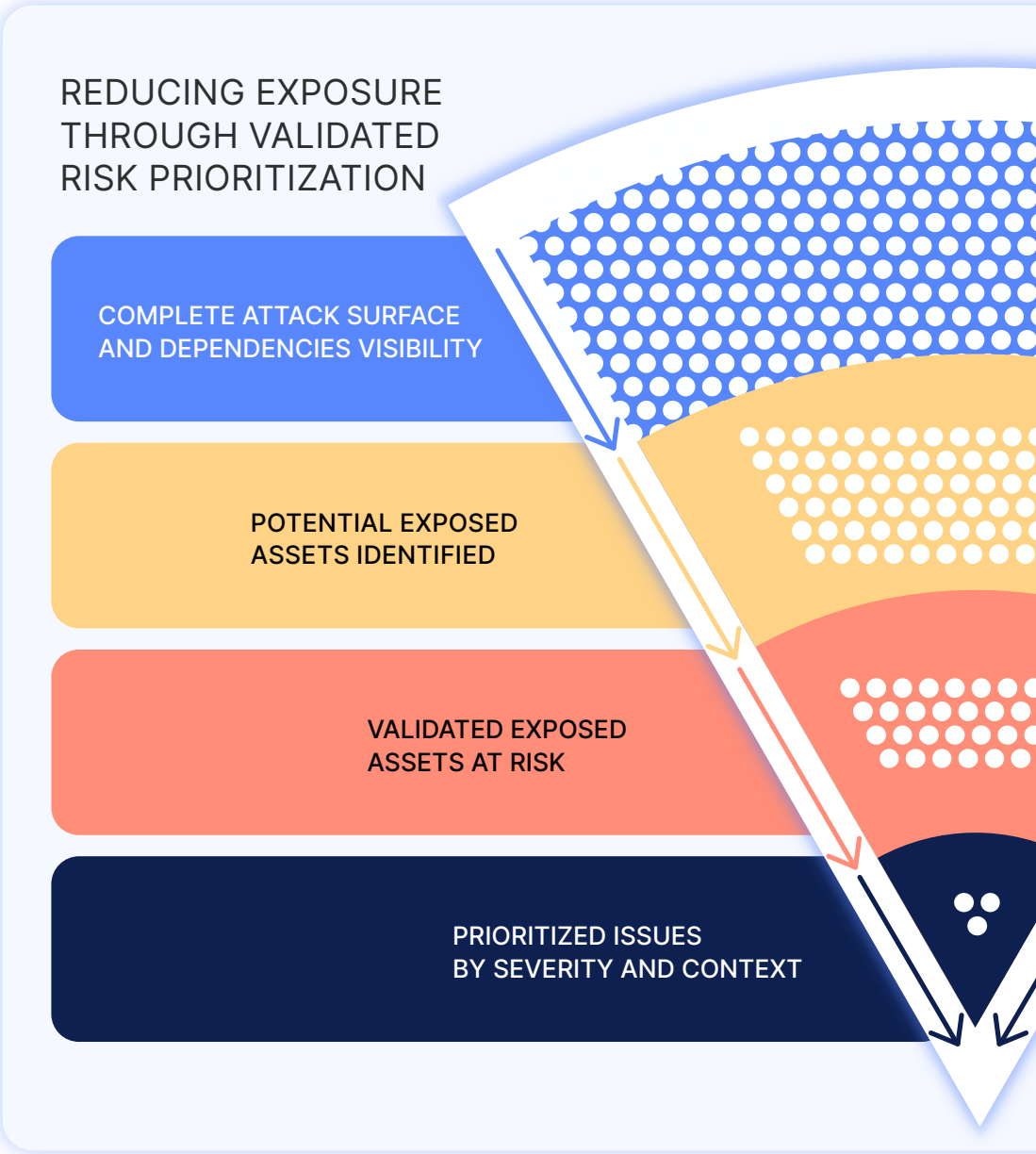
Security posture management is siloed across various infrastructure environments including cloud and IoT, creating critical visibility silos between security teams.

TOO MUCH NOISE

Security teams are overwhelmed by countless alerts and vulnerabilities, making it impossible to focus on what truly matters.

REMEDIATION OPERATIONALIZATION

Organizations often struggle to translate security findings into actual improvements.



HOW IONIX WORKS

IONIX TRANSFORMS THE WAY ORGANIZATIONS HANDLE THE OVERWHELMING CHALLENGE OF MANAGING THEIR EXTERNAL EXPOSURES.

IONIX addresses the growing complexity of vulnerability management by focusing on real threats rather than drowning in potential vulnerabilities. At its core, IONIX bridges the gaps in traditional security approaches through a powerful combination of discovery, validation, and remediation.

With unified visibility across all infrastructure environments, IONIX eliminates the silos that traditionally fragment security teams' view of their attack surface. It continuously maps the entire attack surface from an attacker's perspective, uncovering hidden assets and attack paths that conventional tools miss.

IONIX actively validates which exposures pose real threats in the specific environment. This validation-first approach dramatically reduces alert fatigue while ensuring resources focus on genuine risks.

Upon identifying critical issues, IONIX enhances security team efficiency. It does this by either pinpointing choke points where a specific fix can address multiple vulnerabilities, or grouping issues by asset ownership or team responsibilities. These consolidated findings are then routed through existing security tools and ticketing systems, accelerating remediation.

The result is a transformed security operation where teams move from reactive firefighting to proactive defense, armed with clear, actionable intelligence about the threats that truly matter to their organization.

HOW IONIX WORKS

DISCOVERY

MAP YOUR COMPLETE ATTACK SURFACE

The IONIX multi-layered discovery engine maps an organization's attack surface from an attacker's perspective, complemented by integrations with cloud platforms, CSPM and other security tools. Through advanced machine learning, it performs comprehensive global event tracking, FQDN and IP discovery, and intelligent reverse indexing across domains and cloud platforms. IONIX maps asset connectivity, evaluating potential attack paths while eliminating false positives through evidenced-based attribution of each asset.

INVENTORY

KNOW TRUE SECURITY RISKS BEFORE ATTACKERS DO

IONIX performs deep analysis of discovered assets, determining asset types and identifying the software they run. The platform extracts vulnerability data from the National Vulnerability Database (NVD) to match software versions against known vulnerabilities, creating a dynamic catalog of the external attack surface. This comprehensive inventory establishes the foundation for proactive security management and continuous risk assessment.

ASSESSMENT

UNCOVER SECURITY GAPS

IONIX examines multiple security dimensions of each asset, identifying potential risks. The platform analyzes IT hygiene issues, scans for open ports, and detects misconfigurations and additional security gaps identified in the OWASP Top 10, along with advanced web attack scenarios. This thorough assessment approach delivers clear, actionable insights about assets' security posture to provide an initial risk posture assessment.

VALIDATION

ENSURE TRUE EXPOSURE

IONIX conducts active, non-intrusive security tests that simulate external attacks across the entire attack surface. Without disrupting operations, the platform tests for thousands of risks and continuously expands coverage in response to emerging threats. This validation process identifies critical exposures to enable focus on real exposures rather than handling theoretical risks.

PRIORITIZATION

TRANSFORM VALIDATED RISKS INTO ACTIONABLE INSIGHTS

IONIX intelligent prioritization analyzes critical factors to determine true risk levels such as technical severity, asset importance, and potential blast radius of successful exploits. IONIX prioritizes validated risks, using Intelligent clustering consolidates tasks with common root causes, bundles technically related issues, and groups findings by responsible teams - minimizing redundancy and optimizing remediation efficiency. This strategic approach ensures resources focus on the most critical issues threatening the organization.

REMEDIATION

ACCELERATE RISK DISCOVERY TO RESOLUTION

IONIX transforms security findings into immediate actions and forwards it to the right person. The platform provides clear documentation of asset ownership and exploitation proof. Using various integrations to SIEMs, ticketing systems and more, the right team can be notified and address the risks. This structured approach ensures the highest-impact fixes are prioritized while maintaining clear communication channels throughout the security lifecycle.

”We ultimately chose IONIX because of its ability to go beyond vulnerability detection and into automatic active protection that mitigated the risk of hijacking any of the company’s domains”

CISO,
Fortune 500 Company

GET STARTED TODAY

Contact our team to get a free scan.

Get a free scan | Learn more at ionix.io

DATASHEET IONIX